Akamai DNS Integration Guide

CertSecure Manager uses Akamai as a DNS provider to complete ACME DNS-01 domain validation for automated certificate issuance and renewal.

Prerequisites

- CertSecure Manager deployed and reachable, with administrator access to Utilities → ACME.
- An Akamai Control Center account with permission to create API clients (Identity & Access Management).
- The target domain's zone hosted in Akamai Edge DNS, with authority to create and delete TXT records.
- Outbound HTTPS connectivity from CertSecure Manager to the Akamai API endpoint and to the ACME CA.
- An ACME profile configured for the issuing CA (Let's Encrypt or Google Public CA).

Step 1: Create an Akamai API Credential

- In Akamai Control Center → Identity & Access Management, create an API client with EdgeGrid credentials.
- Authorize the client for Edge DNS – Zone Record Management (read/write) on the relevant zone(s).
- Record the EdgeGrid credentials: client token, client secret, access token, and host.

Note: Akamai Edge DNS uses four EdgeGrid values rather than a single token. Confirm how CertSecure's API Token field expects them for Akamai (e.g. a combined credential string) against the live Add Domain form. The credential must permit TXT record create/delete.

Step 2: Add the Domain in CertSecure Manager

- Go to: Utilities → ACME → Domain.
- Click + Add Domain and fill in:
  - Domain: the FQDN managed in Akamai (e.g. example.com)
  - Provider: Akamai
  - API Token: the Akamai credential from Step 1
- Click Save.

Step 3: Validate DNS Ownership

- Use the Validate action on the domain entry to trigger a DNS-01 check - CertSecure creates and removes a TXT record via the Akamai API.
- When successful, the Validation column shows Valid. Domains must be Valid before certificate issuance.

Step 4: Use in ACME Issuance

- The validated Akamai-managed domain can now be selected by ACME profiles (Let's Encrypt, Google Public CA) for automated DNS-01 issuance and renewal.